Digital Whisper
Technologic Papers

קריפטוגרפיה - חלק ב'

מאת אופיר בק

הקדמה

לפני שנמשיך, אני רוצה לציין את **דניאל ליטבק וסופי אוסמולבסקי**, שהם היחידים שפיצחו את הצופן מהפעם הקודמת. הטקסט המוצפן היה חלק מהעמוד הראשון של כתבו של אל-קינדי, מתמטיקאי ערבי שהיה בין אלו שאחראים לכך שידועה לנו היום התדירות של כל אחת מהאותיות. קיבלתי כעשרה מיילים מאנשים שחשבו שהצליחו לפצח את הצופן, אבל רק דניאל וסופי הצליחו, וממש לפני מועד סגירת הגיליון.

בנוגע לשיטה בה הם עבדו, הם השתמשו בסקריפט של פיית'ון כדי לספור את האותיות, רשמו לעצמם הערות, והשתמשו בניתוח התדירויות כדי להתחיל. לאחר מכן, השלימו מילים ברורות (כמו אלו שדיברנו עליהן בפעם הקודמת) וכך הצליחו לבסוף לפצח את הצופן.

בחלק הקודם עסקנו בצופן הקיסר, שהוא צופן מונואלפביתי. בנוסף לצופן המונואלפביתי הבסיסי ביותר, שהוא צופן הקיסר, יש גם נומנקלטורים (Nomenclature). נומנקלטור הוא מערכת הצפנה שמשלבת קוד וצופן. יש מערכת של 26 אותיות, אך בנוסף אליהן יש מילים שיש להם סימנים משל עצמן, ומשתמשים בסימנים האלו כדי לתאר את המילים האלו, מה שמקשה מעט על הפיצוח. בנוסף, ניתן להוסיף לנומנקלטור "כלומים" (nulls), שהם סימנים שלא מסמלים כלום ונמצאים שם רק בשביל להטעות.

למרות שההצפנה הזו נראית מסובכת, היא לא מסובכת יותר לפיצוח מאשר צופן קיסר, לפחות לא באופן משמעותי. ניתן להשתמש באופן רגיל בניתוח תדירויות, ולאחר מכן לזהות את הסימנים הנוספים על פי ההקשר.

צופן ויז'נר

צופן ויז'נר היה הדור הבא של ההצפנה, והוא פותח באופן שלם רק במאה ה-16. הרקע הוא יחסית פשוט. לאחר פיצוח צופן הקיסר, ניסו מפתחי הצפנים שיטות שונות לפתח צפנים חדשים, שיהיו קשים באופן משמעותי. אחת הדוגמאות היה שימוש ב**צופן פוליאלפביתי**, כלומר, צופן שמשתמש ביותר מסט אחד של אותיות. דוגמה בסיסית שלו הייתה שימוש בשני צפני קיסר, כאשר את הראשון נפעיל על האות הראשונה, ואת השני על האות השנייה, נחזור לראשון לאות השלישית, ולאות הרביעית נשתמש בסט השני, וכן הלאה. הצופן הזה פוצח גם הוא בקלות יחסית, אך ממנו שאב ויז'נר את ההשראה לצופן שלו.

ויז'נר הציע שימוש ב-26 סטים של צופן קיסר, והציב אותם בטבלה, שנקראת "ריבוע ויז'נר":

היסט	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	v	u	w	x	y	z
1	**B**	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	**C**	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	**D**	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	**E**	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	**F**	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	**G**	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	**I**	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	**J**	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	**K**	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	**L**	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	**M**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	**N**	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	**O**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	**P**	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	**Q**	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	**R**	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	**S**	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	**T**	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	**U**	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	**V**	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	**W**	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	**X**	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	**Y**	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	**Z**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	**A**	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

הרעיון הוא שבעזרת ריבוע ויז'נר קל מאוד להצפין אותה בצורה פוליאלפבתית. אם נצפין את האות a לפי האות C, ניגש לשורה השנייה, ונראה שהערך של a יהיה C. אם נצפין את האות f לפי האות G, נפנה לשורה שמתחילה באות G, ונמצא ש-f שווה ל-L. אם השולח משתמש רק באות אחת למפתח שלו, יתקבל צופן מונואלפביתי סטנדרטי, אך כשמשתמשים במפתחות בני כמה אותיות ניתן לראות את השימוש של הצופן. כדי להדגים זאת, נבחר במפתח WHITE, ונצפין את המשפט divert troops to east ridge ונסיר את הרווחים. כדי להשתמש במפתח, נצפין כל אות מהמסר לפי האות במפתח, כאשר את הראשונה נצפין לפי W, את השנייה לפי H וכן הלאה, ולאחר מכן נחזור ל-W שוב. המשפט המתקבל הוא:
.ZPDXVPAZHSLZBHIWZBKMZNM

שימו לב שבעוד ה-Z הראשונה מצפינה את האות d, ההופעה השנייה שלהם מייצגת בכלל את האות r. אם כן, אין ספק שהצופן חסין לניתוח תדירויות סטנדרטי. למרות זאת, הצופן לא נכנס לשימוש מיד לאחר המצאתו, מכיוון שביחס לצפנים אחרים, הוא היה קשה לשימוש, וגזל זמן רב כדי להצפין כל הודעה. לכן,

חיפשו מפתחי הצפנים צופן ברמת ביניים, שמצד אחד לא יגזול זמן רב כל כך, ומצד שני לא יהיה חשוף כמו הצופן המונואלפביתי הישן. במשך למעלה מ-200 שנים, נחשב הצופן ל-**le chiffre indéchiffrable**, או בעברית - 'הצופן שלא ניתן לפצח'. לפני שנגיע לפיצוח של צופן ויז'נר, נחקור קצת את הצפנים שבהם השתמשו בתקופה שלאחר המצאתו של ויז'נר, כשמצאו סוג צופן שיענה על הציפיות שלהם.

הצופן שענה על הציפיות היה הצופן ההומופוני.

צופן הומופוני

צפנים הומופוניים פועלים בצורה מעט שונה מאשר הצופן המונואלפביתי שהזכרנו קודם. אם אתם זוכרים את הטבלה של תדירות האותיות בחלק הקודם, וגם אם לא, האות e היא בעלת התדירות הגבוהה ביותר, והיא מהווה כמעט 12% מהשימוש. הרעיון של צופן הומופוני הוא שימוש במספר סמלים כדי לגלם כל אות, לפי התדירות של האותיות, כלומר, האות e, שמהווה כמעט 12%, תקבל 12 סמלים שונים, כאשר בכל פעם ישתמשו באחד מהם באופן אקראי. האות z לעומת זאת, מהווה מעט פחות מאחוז אחד מהשפה, ולכן היא תקבל רק סמל אחד. כאשר נעשה זאת לכל האותיות, נגרום לכך שלכל סמל תהיה תדירות של 1% בערך, מה שיגרום לצופן להיות חסין לניתוח תדירויות.

עם זאת, הצופן ההומופוני לא היה חסין לחלוטין למפצח מתוחכם. כפי שציינו לפני כן, בניתוח תדירויות אנו משתמשים גם ב'אישיות' של כל אות, ומנצלים תכונות אודות השימוש שלה כדי לזהות את הערך שלה. כדי לפצח את הצופן ההומופוני משתמשים באות q. האות q מופיע באנגלית כשלאחריה תמיד יש את אותה אות, u. ניתן להניח שלאות u יהיו שלושה סמלים, מכיוון שהיא מהווה כ-3% מהשפה האנגלית, ולכן כל מה שצריך לעשות הוא לחפש סמל שלאחריו תמיד מופיעים רק אחד משלושה סמלים שונים, וכך נחשוף כבר שתי אותיות, מהן נוכל להתקדם, תוך ניצול עובדות נוספות.

אופציה נוספת לצופן הומופוני הוא תיאור זוגות של אותיות, המכונים דגרפים (digraphs). באנגלית יש 676 זוגות כאלו, מה שגורם לכך שקשה מאוד לפענח את הצופן. צופן דומה לזה היה "הצופן הגדול", בו השתמש לואי הארבעה-עשר והצופן נשאר סודי במשך שנים רבות מאוד. בצופן הגדול, כל סימן היה בעל ערך של הברה כלשהי, כשבסך הכל היו 576 סימנים שונים בשימוש. חלקם אפילו ביטלו את המשמעות של ההברה הקודמת, מה שהקשה מאוד על הפיצוח.

פיצוח צופן ויז'נר:

במאה ה-19, אותגר צ'רלס באבאג' בידי רופא שחשב שגילה צופן חסין לחלוטין, אך בעצם רק 'גילה מחדש' את צופן ויז'נר. באבאג' ציין כי הצופן הוא לא חדש אלא ישן, ולמרות שלא פוענח עד כה, הוא לא המצאה חדשה. בתגובה להודעה של באבאג', הרופא אתגר את באבאג' להצליח לפענח מסר שהצפין:

```
W U B E F I Q L Z U R M V O F E H M Y M W T
I X C G T M P I F K R Z U P M V O I R Q M M
W O Z M P U L M B N Y V Q Q Q M V M V J L E
Y M H F E F N Z P S D L P P S D L P E V Q M
W C X Y M D A V Q E E F I Q C A Y T Q O W C
X Y M W M S E M E F C F W Y E Y Q E T R L I
Q Y C G M T W C W F B S M Y F P L R X T Q Y
E E X M R U L U K S G W F P T L R Q A E R L
U V P M V Y Q Y C X T W F Q L M T E L S F J
P Q E H M O Z C I W C I W F P Z S L M A E Z
I Q V L Q M Z V P P X A W C S M Z M P R V G
V V Q S Z E T R L Q Z P V J A Z V Q I Y X E
W W O I C C G D W H Q M M V O W S G N T J P
F P P A Y B I Y B J U T W R L Q K L L L M D
P Y V A C D C F Q N Z P I F P P K S D V P T
I D G X M Q Q V E B M Q A L K E Z M G C V K
U Z K I Z B Z L I U A M M V Z
```

למרות שתגובותו של הרופא לא באמת קשורה לטענתו של צ'ארלס באבאג', הוא החליט להיענות לאתגר. לפני שנגיע לפיצוח של הצופן עצמו, נעסוק ברעיון שמאחוריו. הרעיון שעלה בראשו של צ'ארלס באבאג' הוא שימוש בחזרה של המפתח לטובתו. כדי להדגים זאת נשתמש במילת המפתח KING במשפט:

the sun and the man in the moon.

ההצפנה של המשפט הזה תהיה:

```
D P R Y E V N T N B U K W I A O X B U K W W B T
```

המילה the מוצפנת כ-DPR במקרה הראשון, BUK בפעם השנייה, וגם בפעם השלישית BUK. הסיבה לכך היא שבין ה-the השני לבין השלישי יש מרחק של 8 אותיות, שהן בדיוק פעמיים מילת המפתח, מה שגורם לכך שההצפנה חוזרת על עצמה.

על פי שיטתו של באבאג', השלב הראשון בניתוח הוא לחפש רצפים של אותיות המופיעים יותר מפעם אחת בטקסט המוצפן.

יש שתי דרכים בהם זה יכול להתרחש:

1. מדובר באותו רצף שחוזר על עצמו ומשתמש באותו המפתח.
2. רצפים שונים של אותיות הוצפנו בחלקים שונים של המפתח, ובמקרה יצרו רצף זהה.

האפשרות השנייה קלושה ביותר, במיוחד אם נגביל את עצמנו לרצפים של 4 תווים או יותר. בטבלה שלפניכם מופיעים הרצפים, המרווחים ביניהם והמספרים בהם מתחלקים המרווחים:

הרצף	מרווח	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
EFIQ	95				V														V	
PSDLP	5				V															
WCXYM	20	V		V	V					V										V
ETRL	120	V	V	V	V	V		V		V		V			V				V	

השלב הבא הוא לזהות את אורך המפתח. היות והמספר היחיד שמשותף לכולם הוא 5, ניתן לקבוע שאורך המפתח הוא 5.

לעת עתה, נכנה את מלת המפתח K1-K2-K3-K4-K5, כך ש-K1 מייצג את האות הראשונה במילת המפתח וכן הלאה. האות K1 מגדירה שורה אחת בריבוע ויז'נר ולמעשה מספקת אלף-בית להצפנה באמצעות החלפה מונואלפביתית, שפועל על האותיות הראשונה, השישית, האחת-עשרה... של ההודעה. עכשיו, ניתן לבצע ניתוח תדירויות בעזרת גרף עמודות, ולחפש רצפים חוזרים (לעיתים יש סטייה סטטיסטית בגרף) של גובה עמודות. בד"כ מסתמכים על ה"עמק" בגרף בין האותיות Y ל-D, שמופיע לאחר שלוש פסגות ב- V-W-X. בעזרת מציאת המאפיינים המיוחדים האלה, ניתן לדעת כמה הסטות בוצעו, לפי המיקום המקורי של האות V, ביחס לפסגה הראשונה ברצף המוסט. כך מגלים לדוג', שהאות הראשונה היא E, ולאחר בדיקה של האותיות השנייה, השביעית, השתים-עשרה... של ההודעה מגלים את האות השנייה - M. כך ממשיכים עד שמגלים את כל האותיות ומקבלים את מילת המפתח EMILY. על ידי פענוח הטקסט והפרדת המילים אנו מקבלים את הטקסט:

Sit thee down, and have no shame,
Cheek by jowl, and knee by knee:
What care I for any name?
What for order or degree?
Let me screw three up a peg:
Let me loose thy tongue with wine:
Callest thou that thing a leg?
Which is thinnest? Thine or mine? ...(יש המשך)

אלה הם בתים משיר שקרא The Vision of Sin. שם אשתו של כותב השיר הוא Emily.

הצופן האחרון שנעסוק בו בחלק הזה, הוא צופן המכונה "צופן ספר".

צופן ספר

צופן סופר הוא אינו תצורת צופן כמו צופן המופוני או צופן מונואלפביתי, אלא שם כולל לטקסטים מוצפנים שהמפתח שלהם מיוצג בעזרת טקסט אחר. כדי להסביר זאת לעומק נשתמש במשפט הבא:

This is an example. Do not take it the wrong way.

בעזרת שימוש במספר של כל מילה, ובאות הראשונה של כל מילה, נקבל את ה"מילון" הבא:

1 = t	4 = e	7 = t	10 = w
2 = i	5 = d	8 = i	11 = w
3 = a	6 = n	9 = t	

כמו שניתן לשים לב בקלות, חלק מהאותיות מיוצגות על ידי יותר ממספר בודד. ניתן ליצור כך צופן הומופוני שהמפתח שלו הוא המשפט הזה. כמובן שעדיף להשתמש בקטעי טקסט ארוכים, כדי שיהיו לנו את כל האותיות לשימוש בטקסט המוצפן. אחת מההצפנות הידועות שנעשו ככה היא ההצפנה של אחד מ"קבצי ביל", שידועה בכך שאחד מן הקבצים (יש שלושה) הוצפן בצופן ספר כשהמפתח הוא לא פחות מאשר הכרזת העצמאות של ארה"ב.

גם הפעם אני אתן לכם אתגר לפענוח, והפעם זה יהיה פיצוח של צופן ויז'נר. היות וכבר הסברתי את העקרון שעומד מאחורי הפיצוח, אני מקווה שגם הפעם נוכל להכריז כבר בגיליון הבא (אוקטובר 2016) על המנצח בתחרות.

K	Q	O	W	E	F	V	J	P	U	J	U	U	N	U	K	G	L	M	E	K	J	I	N	M	W	U	X	F	Q	M	K	J	B
G	W	R	L	F	N	F	G	H	U	D	W	U	U	M	B	S	V	L	P	S	N	C	M	U	E	K	Q	C	T	E	S	W	R
E	E	K	O	Y	S	S	I	W	C	T	U	A	X	Y	O	T	A	P	X	P	L	W	P	N	T	C	G	O	J	B	G	F	Q
H	T	D	W	X	I	Z	A	Y	G	F	F	N	S	X	C	S	E	Y	N	C	T	S	S	P	N	T	U	J	N	Y	T	G	G
W	Z	G	R	W	U	U	N	E	J	U	U	Q	E	A	P	Y	M	E	K	Q	H	U	I	D	U	X	F	P	G	U	Y	T	S
M	T	F	F	S	H	N	U	O	C	Z	G	M	R	U	W	E	Y	T	R	G	K	M	E	E	D	C	T	V	R	E	C	F	B
D	J	Q	C	U	S	W	V	B	P	N	L	G	O	Y	L	S	K	M	T	E	F	V	J	J	T	W	W	M	F	M	W	P	N
M	E	M	T	M	H	R	S	P	X	F	S	S	K	F	F	S	T	N	U	O	C	Z	G	M	D	O	E	O	Y	E	E	K	C
P	J	R	G	P	M	U	R	S	K	H	F	R	S	E	I	U	E	V	G	O	Y	C	W	X	I	Z	A	Y	G	O	S	A	A
N	Y	D	O	E	O	Y	J	L	W	U	N	H	A	M	E	B	F	E	L	X	Y	V	L	W	N	O	J	N	S	I	O	F	R
W	U	C	C	E	S	W	K	V	I	D	G	M	U	C	G	O	C	R	U	W	G	N	M	A	A	F	F	V	N	S	I	U	D
E	K	Q	H	C	E	U	C	P	F	C	M	P	V	S	U	D	G	A	V	E	M	N	Y	M	A	M	V	L	F	M	A	O	Y
F	N	T	Q	C	U	A	F	V	F	J	N	X	K	L	N	E	I	W	C	W	O	D	C	C	U	L	W	R	I	F	T	W	G
M	U	S	W	O	V	M	A	T	N	Y	B	U	H	T	C	O	C	W	F	Y	T	N	M	G	Y	T	Q	M	K	B	B	N	L
G	F	B	T	W	O	J	F	T	W	G	N	T	E	J	K	N	E	E	D	C	L	D	H	W	T	V	B	U	V	G	F	B	I
J	G	Y	Y	I	D	G	M	V	R	D	G	M	P	L	S	W	G	J	L	A	G	O	E	E	K	J	O	F	E	K	N	Y	N
O	L	R	I	V	R	W	V	U	H	E	I	W	U	U	R	W	G	M	U	T	J	C	D	B	N	K	G	M	B	I	D	G	M
E	E	Y	G	U	O	T	D	G	G	Q	E	U	J	Y	O	T	V	G	G	B	R	U	J	Y	S									

לסיכום

למדנו על מספר צפנים נוספים, בהם גם צפנים הומופוניים (כגון הצופן הגדול) וצפנים פוליאלביתים (כמו צופן ויז'נר). למדנו איך לפצח את צופן ויז'נר, ודיברנו קצת על צפני ספר. בפעם הבא נעסוק בהצפנה מודרנית, ובהצפנות בעידן המחשוב.

על המחבר

שמי אופיר בק, בן 16 מפתח תקווה. אני לומד בתכנית גבהים של מטה הסייבר הצה"לי וב-C-security, לאחר שסיימתי את לימודי המתמטיקה והאנגלית בכיתה י'. קשה למצוא חומר מעודכן בעברית, ולאחר שהמגזין הזה היווה עבורי מקור מידע נגיש, רציתי לתרום חזרה. אני מקווה שנהניתם מהמאמר.

ניתן ליצור איתי קשר בכתובת ophiri99@gmail.com.

קישורים לקריאה נוספת

- **צופן ספר:**

https://en.wikipedia.org/wiki/Book_cipher

- **קבצי בייל:**

https://en.wikipedia.org/wiki/Beale_ciphers